CLAIMS

1. An information security apparatus that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the information security apparatus comprising:

a private key generating unit operable to generate a private key;

a parameter receiving unit operable to receive parameters which respectively determine conditions; and

a public key generating unit operable to generate, with use of the private key, public keys from sets of integers that satisfy the conditions determined by the parameters.

2. The information security apparatus of Claim 1, wherein

the information security apparatus is connected to servers via a network,

the parameters are received from the servers respectively and are different from each other, and

the public key generating unit generates public keys which are different from each other, with use of the respective parameters.

3. The information security apparatus of Claim 2, further comprising:

a public key transmission unit operable to transmit the

public keys to respective source servers that are sources of the respective parameters;

a public key certification receiving unit operable to receive public key certifications from the respective servers, each public key certification including each public key and a signature of each server; and

a key storage unit operable to store the private key and the public key certifications.

4. The information security apparatus of Claim 3, further comprising:

a contents request unit operable to read out one of the public key certifications from the key storage unit, and transmit a contents request that includes the read-out public key certification to a source server that has issued the read-out public key certification; and

a contents acquiring unit operable to acquire contents from the source server in a safe and reliable manner with use of the private key and the public key included in the read-out public key certification.

5. The information security apparatus of Claim 4, wherein the contents acquiring unit includes:

an authenticating unit operable to transmit, to the source server, signature data that is generated with use of the private key and to be authenticated by the source server with use of the public key, and authenticate the source server;

a key sharing unit operable to share key information with the source server if the authentication performed by the authentication unit succeeds;

a receiving unit operable to receive encrypted contents, which are encrypted based on the key information, from the source server; and

a decrypting unit operable to decrypt the encrypted contents based on the key information.

6. The information security apparatus of Claim 3, wherein

the key storage unit is a portable memory card that is inserted in the information security apparatus,

the public key generating unit writes the private key and the public key certifications into the potable memory card, and

the portable memory card includes a secure storage area that is secure against tampering and cryptanalysis from outside, and stores the private key in the secure storage area.

7. The information security apparatus of Claim 6, further comprising:

a memory card authenticating unit operable to authenticate the memory card when the memory card is inserted into the information security apparatus; and

a write-inhibit unit operable to inhibit the public key generating unit from writing the private key and the public key certifications into the memory card if the authentication performed by the memory card authenticating unit fails.

8. The information security apparatus of Claim 1, wherein security of the information security apparatus is based on an elliptic curve discrete logarithm problem,

the parameter receiving unit receives parameters that constitute an elliptic curve, and

the public key generating unit generates the public keys by performing, for each parameter, a multiplication with use of the elliptic curve on the private key.

9. The information security apparatus of Claim 8, wherein the private key generating unit generates a private key *SK*,

the parameter receiving unit receives sets of parameters, each including *a* and *b* constituting the elliptic curve $y^2=x^3+ax+b$, a prime number *p*, and a base point *G* on the elliptic curve, and

the public key generating unit generates the public keys by calculating *SK*G(mod p)* for each set of the parameters.

10. The information security apparatus of Claim 1, wherein security of the information security apparatus is based on an RSA cryptosystem,

the private key generating unit generates a private key *d*,

the parameter receiving unit receives sets of prime numbers *(P, Q)* as the parameters, and

the public key generating unit generates sets of the public

keys *(N, e)* by calculating *N=PQ* and further calculating e from *ed≡1mod(P-1)(Q-1)*, for each set of the prime numbers.

11. A memory card that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the memory card comprising:

a private key generating unit operable to generate a private key;

a parameter receiving unit operable to receive parameters which respectively determine conditions;

a public key generating unit operable to generate, with use of the private key, public keys from sets of integers that satisfy the conditions determined by the parameters, and

a private key storage unit operable to store the private key in an area that is secure against tampering and cryptanalysis from outside.

12. The memory card of Claim 11, wherein

the memory card is inserted in a terminal device that is connected to servers via a network,

the parameters are received from the servers respectively via the terminal device and are different from each other, and

the public key generating unit generates public keys which are different from each other, with use of the respective parameters.

13. The memory card of Claim 12, wherein

the memory card acquires, in a safe and secure manner, contents from each server via the terminal device, with use of the private key and the public keys.

14. An information security system that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the information security apparatus comprising:

a private key generating unit operable to generate a private key;

a parameter receiving unit operable to receive parameters which respectively determine conditions; and

a public key generating unit operable to generate, with use of the private key, public keys from sets of integers that satisfy the conditions determined by the parameters.

15. A key generating method used for an information security apparatus that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the key generating method comprising steps of:

generating a private key;

receiving parameters which respectively determine conditions; and

generating, with use of the private key, public keys from sets of integers that satisfy the conditions determined by the

parameters.

16. A key generating program used for an information security apparatus that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the key generating program comprising steps of:

generating a private key;

receiving parameters which respectively determine conditions; and

generating, with use of the private key, public keys from sets of integers that satisfy the conditions determined by the parameters.

17. A computer-readable recording medium having recorded thereon a key generating program used for an information security apparatus that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition, the key generating program comprising steps of:

generating a private key;

receiving parameters which respectively determine conditions; and

generating, with use of the private key, public keys from sets of integers that satisfy the conditions determined by the parameters.